IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

ANTHONY GEORGES, on behalf of himself and all others similarly situated, Plaintiff, v. **BELLE TIRE DISTRIBUTORS, INC.**, Defendant.	Case No.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Anthony Georges ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Belle Tire Distributors, Inc. ("Defendant" or "Belle Tire"), based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents as to all other matters:

I. Introduction

1. This class action arises out of the recent targeted cyberattack and data breach on Belle Tire's network that resulted in unauthorized access to highly sensitive information pertaining to current and former employees of Defendant. Plaintiff brings this class action against Belle Tire for its failure to secure and safeguard his and Class members' personally identifiable information ("PII" or "Private Information"). As a result, Plaintiff and Class Members suffered

ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. Belle Tire, based in Southfield, Michigan, is an automotive services company that serves thousands of customers in multiple states.

3. On or about October 31, 2024, Belle Tire filed official notice of a hacking incident with the Office of the Maine Attorney General.

4. On or about the same time, Belle Tire also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice, Belle Tire detected unusual activity on some of its computer systems on June 11, 2024. In response, the company conducted an investigation which revealed that an unauthorized party had access to certain company files on or around the same date (the "Data Breach"). Yet, Belle Tire waited more than three months to notify the public that they were at risk.[1]

[1] The Data Breach was publicly disclosed to the Office of the Maine Attorney General's website, and is available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/45c309c0-e0c4-4802-b8b2-2123c0a5ae4b.html (last accessed Nov. 14, 2024).

6. As a result of this delayed response, Plaintiff and "Class Members" (defined below) had no idea for more than three months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. Belle Tire's notice letter provided scant detail, particularly considering the size and scope of the Data Breach and the sensitivity of Plaintiff's and Class Members' compromised information.

8. Belle Tire's notice did not disclose how it discovered the cybersecurity attack, how the attack was detected and terminated, the means and mechanisms of the cybersecurity attack, the reason for its delay in notifying Plaintiff and the Class of the Data Breach after learning that Private Information was impacted, how Belle Tire determined that PII was "impacted," and, importantly, what steps Belle Tire took following the Data Breach to secure its systems and prevent future cyberattacks.

9. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, current and former employees' name, address, date of birth, Social Security number, and driver's license number that Belle Tire collected and maintained.

10. The Data Breach was a direct result of Belle Tire's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect clients' PII from the foreseeable threat of a cyberattack.

11. By taking possession and control of Plaintiff's and Class Members' Private Information for its own pecuniary benefit, Belle Tire assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' Private Information against unauthorized access and disclosure. Belle Tire also had a duty to adequately safeguard this Private Information under industry standards and duties imposed by statutes, Section 5 of the Federal Trade Commission Act ("FTC Act"). Belle Tire breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect clients' Private Information from unauthorized access and disclosure.

12. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. As a result of the Data Breach, Plaintiff and Class Members are at imminent and substantial risk of experiencing various types of misuse of their Private Information in the coming years, including but not limited to, unauthorized access to email accounts, tax fraud, and identity theft.

13. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take several additional prophylactic measures.

14. There has been no assurance offered by Belle Tire that all impacted Private Information or copies thereof have been recovered or destroyed.

15. As a result of Belle Tire's inadequate security and breach of its duties and obligations, the Data Breach occurred, causing Plaintiff and Class Members to suffer injury and ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from its exposure, emotional distress, and the present and imminent risk of fraud and identity theft caused by the compromise of their sensitive personal information. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Belle Tire, its officials, and its agents—was compromised and unlawfully accessed due to the Data Breach.

16. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential Private Information still remains in the possession of Belle Tire. Absent additional safeguards and

independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

17. Belle Tire disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard client PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt and adequate notice of the Data Breach.

18. In addition, Belle Tire failed to properly monitor the computer network and systems that housed the Private Information. Had Belle Tire properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

19. The security of Plaintiff's and Class Members' identities is now at risk because of Belle Tire's wrongful conduct as the Private Information that Belle Tire collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

20. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Belle Tire, and thus Belle Tire

was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

21. As a result of the Data Breach, Plaintiff and Class Members have been exposed to actual fraud and identity theft as well as a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against further fraud and identity theft.

25. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

22. Plaintiff and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts and medical records for fraud or identity theft. Due to the fact that the exposed information potentially includes Social Security numbers ("SSNs") and other immutable personal details, Plaintiff and Class Members will be at risk of identity theft and fraud that will persist throughout the rest of their lives.

23. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach. Plaintiff and Class Members seek to hold Belle Tire responsible for the harms resulting from the massive and preventable

disclosure of such sensitive and personal information. Plaintiff seeks to remedy the harms resulting from the Data Breach on behalf of himself and all similarly situated individuals whose Private Information was accessed and exfiltrated during the Data Breach.

24. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, and declaratory judgment.

II. THE PARTIES

26. Plaintiff Anthony Georges is a resident and citizen of the State of Michigan.

27. Defendant Belle Tire is an automotive service provider with its principal place of business at 25800 Northwestern Highway, Southfield, Michigan 48075.

III. JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Belle Tire. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

29. This Court has jurisdiction over Belle Tire because Belle Tire is incorporated and conducts business in this District.

30. Venue is proper in this District under 28 U.S.C. §1391(a)(1) because Belle Tire resides in this District and is being served in this District.

IV. FACTUAL ALLEGATIONS

A. Belle Tire's Business and Collection of Plaintiff's and Class Members' Private Information

31. Founded in 1922, Belle Tire is an American tire, wheel and automotive service retailer providing tire repair, alignment, brakes, and other mechanical services.[2] Belle Tire operates more than 175 locations in Michigan, Indiana, Ohio, and Illinois.[3] Belle Tire employs approximately 3,000 individuals and generates approximately $350 million in annual revenue.[4]

32. Because of the highly sensitive and personal nature of the information Belle Tire acquires and stores with respect to its employees, Belle Tire, upon information and belief, promises to, among other things: keep employees' Private Information private; comply with industry standards related to data security and the maintenance of its employees' Private Information; inform its employees of its legal duties relating to data security and comply with all federal and state laws protecting

[2] *See* https://www.linkedin.com/company/belle-tire (last visited Nov. 14, 2024).
[3] *Id*.
[4] *Id*.

employees' Private Information; only use and release employees' Private Information for reasons that relate to the services it provides; not store former employees' Private Information for longer than is necessary to carry out its business operations; and provide adequate notice to its current and former employees if their Private Information is disclosed without authorization.

33. By obtaining, collecting, using, and deriving a benefit from its employees' Private Information, Belle Tire assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

34. Plaintiff and Class Members relied on Belle Tire to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

35. Indeed, Defendant provides on its website that: "Belle Tire Distributors Inc. maintain appropriate physical, digital and procedural protection of personal information."[5]

36. In order to apply to be an employee or obtain certain employment related benefits from Defendant, Plaintiff and Class Members were required to provide sensitive and confidential PII, including their names, contact information, driver's licenses, and Social Security numbers.

[5] https://www.belletire.com/our-company/privacy (last accessed Nov. 14, 2024).

37. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

39. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its employees' PII safe and confidential.

40. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

41. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

43. However, Belle Tire did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited three months to disclose the Data Breach publicly.

B. The Data Breach and Notice Letter

44. In or about November 2024, Defendant began sending Plaintiff and other victims of the Data Breach an "Important Security Notification" letter (the "Notice Letter"), informing them that:

> **What Happened?**
> On June 11, 2024, Belle Tire identified activity in our computer system occurring without our permission. We quickly took steps to stop that activity. We hired a third-party team to investigate and assist us. We also contacted law enforcement. We have since learned that a cybercriminal was able to see and take copies of some data from our computer network. On September 11, 2024, we received more specific information that personal data linked to you may have been seen and taken.
>
> **What Information Was Involved?**
> The data that may have been seen and taken includes contact information (such as name, address, and date of birth) plus one or more of the following: a) Social Security number or, (b) driver's license. The data that may have

been seen and taken was not the same for everyone.[6]

45. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

46. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

47. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted

[6] The "Notice Letter". A sample copy is available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792a1252b4f8318/45c309c0-e0c4-4802-b8b2-2123c0a5ae4b.html

information including Plaintiff's and Class Members' Social Security numbers for download and theft.

48. Defendant failed to specify whether it undertook any efforts to contact the approximate 29,000 Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

49. Due to Belle Tire's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

50. The attacker targeted, accessed, and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiff and Class Members, including their names and Social Security numbers. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

51. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

52. Belle Tire had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

53. Plaintiff and Class Members provided their Private Information to Belle Tire with the reasonable expectation and mutual understanding that Belle Tire would comply with its obligations to keep such information confidential and secure from unauthorized access.

54. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Belle Tire assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

55. Belle Tire's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the across industries preceding the date of the breach.

56. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and Class Members would not have allowed Belle Tire or anyone in Belle Tire's position to receive their Private Information had they known that Belle Tire would fail to implement industry standard protections for that sensitive information.

57. As a result of Belle Tire's negligent and wrongful conduct, Plaintiff's and Class Members' highly confidential and sensitive Private Information was left exposed to cybercriminals.

C. Belle Tire Failed to Comply with FTC Guidelines

58. Belle Tire was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

59. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

60. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their

network's vulnerabilities; and implement policies to correct any security problems.[7] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[8]

61. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from

[7] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 14, 2024).
[8] *Id*.

these actions further clarify the measures businesses must take to meet their data security obligations.

63. Belle Tire failed to properly implement basic data security practices.

64. Belle Tire's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

65. Belle Tire was at all times fully aware of the obligation to protect the Private Information of current and former employees. Belle Tire was also aware of the significant repercussions that would result from its failure to do so.

D. Belle Tire Failed to Comply with Industry Standards

66. Experts studying cyber security routinely identify recruiting services as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

67. Several best practices have been identified that at a minimum should be implemented by staffing companies like Belle Tire, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

68. Other best cybersecurity practices that are standard across industries include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

69. Belle Tire failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. These foregoing frameworks are existing and applicable industry standards in the industry, and Belle Tire failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

E. Belle Tire Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

71. In addition to its obligations under federal and state laws, Belle Tire owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining,

retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Belle Tire owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

72. Belle Tire owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

73. Belle Tire owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

74. Belle Tire owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

75. Belle Tire owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

76. Belle Tire owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

77. Belle Tire owes a legal duty to secure current and former employees' PII and to timely notify them of a data breach.

78. Belle Tire breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Belle Tire's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
b. Failing to adequately protect current and former employees' Private Information;
c. Failing to properly monitor its own data security systems for existing intrusions;
d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
e. Failing to detect unauthorized ingress into its systems;
f. Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;
g. Failing to detect unauthorized exfiltration of the most sensitive data on its systems;
h. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
k. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
l. Failing to adhere to industry standards for cybersecurity as discussed above; and

m. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

79. Belle Tire negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

80. Had Belle Tire remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Belle Tire could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

81. However, due to Belle Tire's failures, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Belle Tire.

F. Belle Tire Knew or Should Have Known that Criminals Target Private Information

82. At all relevant times, Belle Tire knew, or should have known, its clients', Plaintiff's, and all other Class Members' Private Information was a target for malicious actors. Despite such knowledge, Belle Tire failed to implement and maintain reasonable and appropriate data privacy and security measures to protect

Plaintiff's and Class Members' Private Information from cyber-attacks that Belle Tire should have anticipated and guarded against.

83. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of clients and/or like Plaintiff and Class Members.

84. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

85. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target

more victims and offers an incentive for others to get involved in this type of illegal activity."[9]

86. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

87. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

G. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

71. Cyberattacks and data breaches at companies like Belle Tire are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

72. The United States Government Accountability Office released a report

[9] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed November 14, 2024).
[10] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[11]

73. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone

[11] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

calls and text messages or phishing emails.

74. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.

75. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

76. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account

[12] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Nov. 14, 2024).

and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

77. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

78. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[13]

79. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many

[13] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

80. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

81. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

82. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

83. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

[14] *Data Breaches Are Frequent*, *supra* note 11.

84. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [15]

85. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[16]

86. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[17] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a

---

[15] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).
[16] *Id.*
[17] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Nov. 14, 2024).

false identity.[18] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

87. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

88. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Belle Tire is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information,

[18] *Id* at 4.

[19] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

89. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[20] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[21]

90. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[22]

91. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[23]

92. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number,

---

[20] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[21] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[22] *Id.*

[23] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Nov. 14, 2024).

a breach victim has to demonstrate ongoing harm from misuse of his or her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

93. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[24]

94. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

[24] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

95. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[25]

96. Cybercriminals can post stolen Private Information on the cyber black-market for years following a data breach, thereby making such information publicly available.

97. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [26] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[27]

---

[25] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

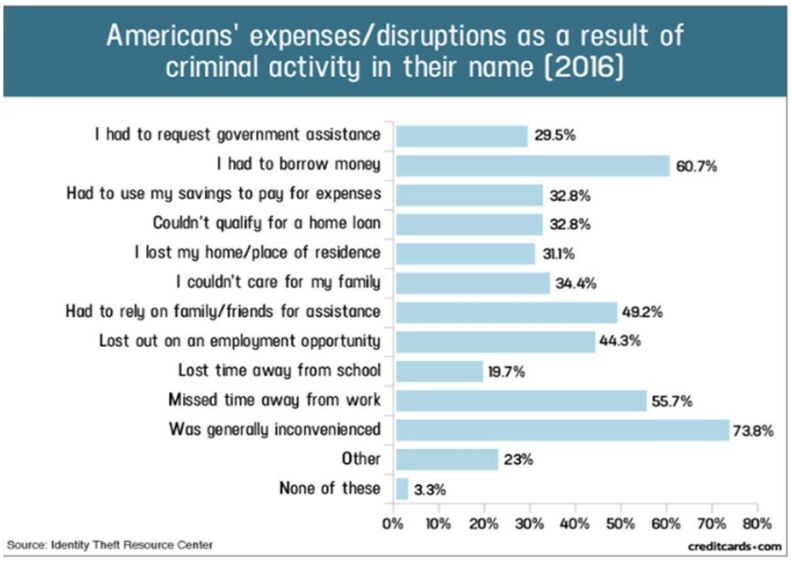
[26] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[27] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

98. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[28]

99. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

100. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



[28] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

101. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[29]

102. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

[29] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

103. Plaintiff and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property, including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Private Information being in the hands of criminals and having already been misused;

e. Damages flowing from Belle Tire's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of clients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

104. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Belle Tire, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Belle Tire has shown itself to be wholly incapable of protecting Plaintiff's and Class Members' Private Information.

105. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to Belle Tire is removed from Belle Tire's unencrypted files.

106. Belle Tire itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members the inadequate 24 months of identity theft protection and credit monitoring services. This limited identity theft monitoring

is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.

107. Belle Tire further acknowledged, in its letter to Plaintiff and Class Members, that, in response to the Data Breach, Belle Tire is "making its computer systems even stronger than before in an effort to prevent this from happening again."

108. The notice further acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous "steps" for Class Members to take in an attempt to mitigate the harm caused by the Data Breach, and that financial harm would likely occur, stating:

> If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

109. At Belle Tire's suggestion, Plaintiff is trying to mitigate the damage that Belle Tire has caused him. Given the kind of Private Information Belle Tire made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have their Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their

lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[30] None of this should have happened.

110. Because of the value of its collected and stored data, Belle Tire knew or should have known about these dangers and strengthened its data security accordingly. Belle Tire was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

H. The Data Breach Was Foreseeable and Preventable

111. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[31] Yahoo,[32]

[30] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[31] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[32] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

Marriott International,[33] Chipotle, Chili's, Arby's,[34] and others.[35]

112. Belle Tire should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

113. Belle Tire was clearly aware of the risks it was taking and the harm that could result from inadequate data security, and it could have prevented this Data Breach.

114. Data disclosures and data breaches are preventable.[36] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[37] She added that "[o]rganizations that collect, use, store, and share sensitive personal data

---

[33] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[34] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[35] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[36] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[37] *Id.* at 17.

must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[38]

115. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[39]

116. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[40] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also

---

[38] *Id.* at 28.
[39] *Id.*
[40] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

117. Upon information and belief, Belle Tire failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Belle Tire also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

118. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[41]

119. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Belle Tire could and should have

[41] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[42]

120. The threat continues. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).

[42] *Id.* at 3-4.

121. Further, to prevent and detect ransomware attacks, Belle Tire could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks[.]

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)[.]

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it[.]

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-

> Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic[.][43]

122. In addition, to prevent and detect ransomware attacks, Belle Tire could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities

---

[43] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[44]

123. Given that Belle Tire was storing the Private Information of more than 29,000 individuals, Belle Tire could and should have implemented all of the above measures to prevent and detect ransomware attacks. These are basic, common-sense email security measures that every business should be doing. Belle Tire, with its heightened standard of care should be doing even more.

124. Specifically, among other failures, Belle Tire had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[45] Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message

[44] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.
[45] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

to these organizations is simple: encryption is your best defense against these incidents."[46]

125. Charged with handling sensitive Private Information Defendant knew, or should have known, the importance of safeguarding Plaintiff's and Class Members' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members after a breach. Belle Tire failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

126. With respect to training, Defendant specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

[46]"Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

127. The Private Information was also maintained on Belle Tire's computer system in a condition vulnerable to cyberattacks, such as through the infiltration of Defendant's systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Belle Tire, and thus Belle Tire was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left it in a vulnerable position.

128. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information.

129. Plaintiff and Class Members entrusted their Private Information to Belle Tire as a condition of receiving recruiting related services. Plaintiff and Class Members understood and expected that Belle Tire or anyone in Belle Tire's position would safeguard their Private Information against cyberattacks, delete or destroy Private Information that Belle Tire was no longer required to maintain, and timely and accurately notify them if their Private Information was compromised.

I. The Monetary Value of Privacy Protections and Private Information

130. The fact that Plaintiff's and Class Members' Private Information was stolen means that Class Members' information is likely for sale by cybercriminals

and will be misused in additional instances in the future. Indeed, there is already evidence that Plaintiff's Private Information is on the dark web.

131. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

132. As discussed above, Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[47]

133. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[48]

[47] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Nov. 14, 2024).

[48] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last accessed Nov. 14, 2024).

134. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[49]

135. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[50]

136. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[51] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private

---

[49] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), https://allthingsd.com/20110228/webs-hot-new-commodity-privacy/ [hereinafter *Web's New Hot Commodity*] (last accessed Nov. 14, 2024).

[50] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last accessed Nov. 14, 2024).

[51] *Web's Hot New Commodity*, *supra* note 17.

Information. This business has created a new market for the sale and purchase of this valuable data.

137. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[52]

138. As discussed above, the value of Plaintiff's and Class Members' Private Information on the black market is substantial.

139. The ramifications of Belle Tire's failure to keep Plaintiff's and Class Members' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

140. Victims may not realize their identity has been compromised until long after it has happened.[53] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim

---

[52] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*] (last accessed November 30, 2022).

[53] *See, e.g.*, *Survey on Medical Identity Theft*, Ponemon Institute, June 2012, https://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf (last accessed Nov. 14, 2024).

of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[54]

141. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

142. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

143. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[55] For example, different PII elements from various sources may be

---

[54] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed Nov. 24, 2024).

[55] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-

able to be linked in order to identify an individual, or access additional information about or relating to the individual.[56] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class Members that was misused.

144. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

145. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in fraudulent activity.

---

staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework (last accessed Nov. 24, 2024).

[56] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

146. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

J. The Data Breach's Impact on Plaintiff and Class Members

147. Belle Tire received Plaintiff's PII as a condition of receiving employment and/or car repair services. In requesting and maintaining Plaintiff's PII for business purposes, Belle Tire expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's PII. Belle Tire, however, did not take proper care of Plaintiff's PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Belle Tire inadequate data security measures.

148. If Plaintiff Georges had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

149. Plaintiff is a former employee of Belle Tire. Plaintiff also was a customer of Defendant, having last obtained services from Defendant on April 27, 2024.

150. In order to obtain employment and/or services from Defendant, Plaintiff was required to provide his Private Information to Defendant.

151. At the time of the Data Breach, Belle Tire retained Plaintiff Georges' Private Information in its system.

152. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

153. Plaintiff became aware of the Data Breach through a data breach notice letter dated October 31, though he received the notice on November 12. On the same day he became aware of the Data Breach, Plaintiff immediately took steps to protect and vindicate his rights, including by initiating this litigation.

154. Plaintiff has already experienced harm from this breach, through multiple unauthorized charges that occurred after the breach occurred and are therefore fairly traceable to it. On July 27, 2024, Plaintiff noticed unauthorized charges on his credit for $8.18 and $16.07. Again on August 28, 2024, Plaintiff noticed unauthorized charges for $25.73 and $23.83. Plaintiff's latest unauthorized charge occurred on September 26, 2024, for $5.00.

155. Belle Tire's conduct, which allowed the Data Breach to occur, caused Plaintiff significant injuries and harm, including but not limited to, the following—Plaintiff immediately devoted (and must continue to devote) time, energy, and money to: closely monitoring bills, records, and credit and financial accounts;

changing login and password information on any sensitive account even more frequently than he already does; more carefully screening and scrutinizing phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; searching for suitable identity theft protection and credit monitoring services and paying for such services to protect themselves; and placing fraud alerts and/or credit freezes on his credit file. Plaintiff has taken or will be forced to take these measures in order to mitigate his potential damages as a result of the Breach.

156. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years, and possibly his entire life. Indeed, Plaintiff has already had to replace a credit card to try to mitigate his risk. Consumer victims of data breaches are more likely to become victims of identity fraud.[57]

157. Plaintiff greatly values his privacy. Plaintiff and Class Members did not receive the full benefit of their bargain when paying for auto services, and instead received services that were of a diminished value. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the

[57] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Nov. 24, 2024).

services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

158. They would not have obtained auto repair services from Belle Tire, or paid the amount they did to receive such, had they known that Belle Tire would negligently fail to adequately protect their PII. Indeed, Plaintiff paid Belle Tire for auto repair services with the expectation that Belle Tire would keep his PII secure and inaccessible from unauthorized parties. Plaintiff and Class Members would not have obtained services had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

159. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff's and Class members' Private Information as detailed above, and Plaintiff and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

160. Plaintiff is also at a continued risk of harm because his PII remains in Belle Tire's system, which has already been shown to be susceptible to compromise

and attack and is subject to further attack so long as Belle Tire fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

161. As a result of the Data Breach, and in addition to the time Plaintiff has spent and anticipates spending to mitigate the impact of the Data Breach on his life, Plaintiff has also suffered emotional distress from the public release of his PII, which he believed would be protected from unauthorized access and disclosure. The emotional distress he has experienced includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing his PII for the purposes of identity theft and fraud.

162. Additionally, Plaintiff has suffered damage to and diminution in the value of his highly sensitive and confidential PII—a form of property that Plaintiff entrusted to Belle Tire and which was compromised as a result of the Data Breach Belle Tire failed to prevent. Plaintiff has also suffered a violation of his privacy rights as a result of Belle Tire's unauthorized disclosure of his PII.

163. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on

their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

164. Some of the injuries and risks associated with the loss of Private Information have already manifested themselves in Plaintiff's and other Class Members' lives, as previously detailed. Each Class Member received a cryptically written notice letter from Defendant stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this Private Information could have gone, or who might have access to it.

165. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

166. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

167. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of

the Data Breach reported by Defendant in November 2024 (the "Class").

In addition, or in the alternative, Plaintiff proposes the following state class:

168. Excluded from the Class are: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

169. Plaintiff reserves the right to amend or modify the Class or Class definitions or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

170. **Numerosity:** The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 29,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine Attorney General's Office. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

171. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Belle Tire unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Belle Tire failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Belle Tire's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Belle Tire's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Belle Tire owed a duty to Class Members to safeguard their Private Information;

f. Whether Belle Tire breached the duty to Class Members to safeguard their Private Information;

g. Whether Belle Tire knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Belle Tire should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Belle Tire's misconduct;

j. Whether Belle Tire's conduct was negligent;

k. Whether Belle Tire breached implied contracts with Plaintiff and Class Members;

l. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

m. Whether Belle Tire failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

172. **Typicality**: Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

173. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

174. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief

that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

175. **Predominance**: Belle Tire has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Belle Tire's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

176. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Belle Tire. In contrast, the conduct of this action as a Class action

presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

177. Belle Tire has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

178. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Belle Tire failed to timely and adequately notify the public of the Data Breach;

b. Whether Belle Tire owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Belle Tire's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Belle Tire's failure to institute adequate protective security measures amounted to negligence;

e. Whether Belle Tire failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

179. Finally, all members of the proposed Class are readily ascertainable. Belle Tire has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Belle Tire.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

180. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

181. Belle Tire required employees and customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

182. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its employees and customers, which solicitations and services affect commerce.

183. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

184. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

185. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

186. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

187. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

188. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and

Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment or services with Defendant.

189. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

190. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

191. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to regulations.

192. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

193. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

194. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures

to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- Failing to adequately monitor the security of their networks and systems;
- Allowing unauthorized access to Class members' PII;
- Failing to detect in a timely manner that Class Members' PII had been compromised;
- Failing to remove former employees' PII it was no longer required to retain pursuant to regulations; and
- Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

195. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

196. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

197. Belle Tire has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

198. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

199. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

200. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

201. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting employers in possession of PII.

202. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

203. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

204. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

205. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

206. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

207. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous

courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

208. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

209. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

210. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

211. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of

the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

212. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

213. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

214. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

215. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

216. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

217. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

218. Plaintiff and Class Members were required deliver their PII to Defendant as part of the process of obtaining employment and/or services with Defendant. Plaintiff and Class Members provided their labor and PII to Defendant with the assumption that a portion of its earnings would be used to adequately safeguard their PII and would not have obtained employment or sought services with Defendant had they known that Defendant's data security practices were substandard.

219. Belle Tire solicited, offered, and invited Class Members to provide their Private Information as part of Belle Tire's regular business practices. Plaintiff and

Class Members accepted Belle Tire's offers and provided their Private Information to Belle Tire.

220. Belle Tire accepted possession of Plaintiff's and Class Members' Private Information for the purpose of performing its regular business operations.

221. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

222. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

223. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from

unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

224. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

225. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

226. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

227. Plaintiff and Class Members provided their Personal Information to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

228. Plaintiff and the Class Members would not have entrusted their Private Information to Belle Tire in the absence of such an implied contract to keep their information reasonably secure.

229. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

230. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

231. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

232. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

233. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

234. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

235. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

236. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring

procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

237. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

238. This count is pleaded in the alternative to Count II (breach of implied contract).

239. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their labor to Defendant and/or its agents and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the employment positions that were the subject of the transactions and should have had their PII protected with adequate data security.

240. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

241. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

242. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

243. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained employment at Defendant.

244. Plaintiff and Class Members have no adequate remedy at law.

245. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

246. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

247. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

248. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful

conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

249. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class)

250. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

251. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

252. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

253. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party. Defendant's acts and omissions giving rise to the Data Breach were intentional in that the

decisions to implement lax security and failure to timely notice Plaintiff and the Class were undertaken willfully and intentionally.

254. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading their privacy by improperly using their PII obtained for another purpose, or disclosing it to unauthorized persons;

c. Failing to adequately secure their PII from disclosure to unauthorized persons; and

d. Enabling the disclosure of their PII without consent.

255. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded and private data.

256. Plaintiff's and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in

Plaintiff's and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

257. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

258. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

259. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

260. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class)

261. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

262. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and common law described in this Complaint.

263. Belle Tire owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

264. Belle Tire still possesses Private Information regarding Plaintiff and Class Members.

265. Plaintiff alleges that Belle Tire's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

266. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Belle Tire owes a legal duty to secure its current and former employees' Private Information from unauthorized disclosure and theft;

b. Belle Tire's existing security measures do not comply with its implicit contractual obligations and duties of care to provide

reasonable security procedures and practices that are appropriate to protect current and former employees' Private Information; and

c. Belle Tire continues to breach this legal duty by failing to employ reasonable measures to secure current and former employees' Private Information.

267. This Court should also issue corresponding prospective injunctive relief requiring Belle Tire to employ adequate security protocols consistent with legal and industry standards to protect current and former employees' Private Information, including the following:

a. Order Belle Tire to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members; and

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Belle Tire must implement and maintain reasonable security measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Belle Tire's systems on a periodic basis, and ordering Belle Tire to promptly

correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Belle Tire's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations; and

viii. meaningfully educating its current and former employees about the threats they face with regard to the security of their Private

Information, as well as the steps Belle Tire's current and former employees should take to protect themselves.

268. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Belle Tire. The risk of another such breach is real, immediate, and substantial. If another breach at Belle Tire occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

269. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Belle Tire if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Belle Tire's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Belle Tire has a pre-existing legal obligation to employ such measures.

270. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Belle Tire, thus preventing future injury to Plaintiff and other current and former employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a) An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b) Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c) An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d) An order instructing Belle Tire to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e) An order requiring Belle Tire to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f) A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g) An award of such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: November 14, 2024

Respectfully submitted,

By: /s/ E. Powell Miller

E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM, P.C.
950 West University Drive
Rochester, MI 48307
Tel: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

Nicholas A. Migliaccio
Jason S. Rathod
MIGLIACCIO & RATHOD LLP
412 H St. NE, Suite 302
Washington, D.C. 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiff and Putative Class